STATE OF ALABAMA

Information Technology Standard

Standard 680-03S1: Encryption

1. INTRODUCTION:

Encryption is a technique used to help protect the confidentiality of stored or transmitted information. As required in this and other State standards, encryption must be utilized to protect sensitive and confidential information. Security Management Plans must address the required level of information protection taking into account the method of encryption used, key management strategies, and the length of cryptographic keys employed.

2. OBJECTIVE:

Provide the minimum requirements for the selection, application, and management of encryption technology.

3. SCOPE:

These requirements apply to sensitive or confidential systems; to sensitive or confidential data accessed, stored, or transmitted on State and public networks; and to sensitive or confidential data recorded or stored on portable devices.

4. REQUIREMENTS:

4.1 ENCRYPTION UTILIZATION

Policy: Utilize encryption to protect sensitive and confidential systems and information as required in applicable State standards.

Use encryption to protect sensitive and confidential systems and information as specified in this and other applicable standards and when other controls do not provide adequate protection.

Users accessing sensitive and confidential systems or information from outside State or agency networks must encrypt the session.

Encrypt sensitive and confidential data on portable data storage devices (PDA, laptop, flash drive, CD, DVD, or any other external storage device).

Devices that do not support encryption shall not be used for non-temporary storage of sensitive or confidential data; transfer data to secure storage as soon as practical. Secure the portable device using some physical security method, and when possible store the memory unit separately from the device used to create the data (e.g., digital cameras: store the camera and the memory card in separate secure locations when the camera is not in use).

4.2 ENCRYPTION METHODS

Policy: State encryption technologies shall use proven industry standard algorithms specified in applicable State standards to be reviewed annually and upgraded as necessary.

The use of proprietary encryption algorithms, an algorithm that has not been made public and/or has not withstood public scrutiny (regardless of whether the developer of the algorithm is a vendor, an individual, or the government) is not allowed for any purpose.

Whenever possible, encryption products used should be validated by the NIST Cryptographic Module Validation Program (CMVP) and be listed on the FIPS 140-2 Cryptographic Module Validation List. These requirements aid in providing a trusted computing base for encryption services which are essential for maintaining the confidentiality of the information these systems process.

4.2.1 Acceptable Methods

Encryption methods that utilize either the Triple Data Encryption Standard (Triple DES) or the Advanced Encryption Standard (AES) are acceptable. Encryption methods shown below can also be used to protect sensitive and confidential information:

- Virtual Private Network (VPN) – allows information to be sent securely between two end stations or networks over an un-trusted communications medium; use of VPN technology is the preferred method for securing sensitive and confidential communications.
- IPSEC- is suitable for all types of Internet Protocol (IP) traffic, and may be used to secure Internet and other IP communications within State and agency networks and to connect to authorized external customers.
- Secure Sockets Layer (SSL) – may be deployed to provide secured access to sensitive and confidential information on Web servers.
- Secure Shell (SSH) – may be utilized for the remote administration of sensitive systems.

Other methods of encryption require explicit approval of the State IT Security Council before being used to protect State data or systems.

4.2.2 Unacceptable Methods

Unacceptable methods of encryption include:

- Data Encryption Standard (DES)
- Wired Equivalent Privacy (WEP)

4.3 KEY LENGTH

Policy: Minimum cryptosystem key lengths shall be specified in applicable State standards to be reviewed annually and upgraded as necessary.

Symmetric cryptosystems (such as AES) require a minimum 128 bit key length.

Asymmetric cryptosystems (such as RSA) require key lengths equivalent to a 128 bit or longer symmetric key. Example: A 3072-bit RSA key is equivalent to a 128-bit symmetric key.

The State IT Security Council shall conduct annual review of key length and other encryption requirements when scheduled to conduct the annual review of this standard.

5. DEFINITIONS:

AES: Symmetric block cipher algorithm using cryptographic key sizes of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. WPA2 is an implementation of AES.

ASYMMETRIC CRYPTOSYSTEM: A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (public-key encryption).

DES: Cryptographic algorithm designed for the protection of unclassified data and published by the National Institute of Standards and Technology (NIST) in Federal Information Processing Standard (FIPS) Publication 46. DES only supports key lengths of 56 bits which is considered inadequate.

RSA: An asymmetric key encryption algorithm based on factoring very large integers. Asymmetric algorithm keys must be longer for equivalent resistance to attack than symmetric algorithm keys. 1024-bit RSA keys are equivalent in strength to 80-bit symmetric keys, 2048-bit RSA keys to 112-bit symmetric keys and 3072-bit RSA keys to 128-bit symmetric keys. RSA are the initials of the three algorithm creators: Rivest, Shamir, and Adleman.

SSH: Secure Shell (SSH), a computer program and an associated network protocol designed for logging into and executing commands on a networked computer, provides secure encrypted communications between two untrusted hosts over an non-secure network. SSH is most commonly used in combination with SFTP, as a secure alternative to FTP or in combination with SCP, as a secure alternative for rcp file transfers in Unix environments.

SYMMETRIC CRYPTOSYSTEM: A method of encryption in which the same key is used for both encryption and decryption of the data (secret key encryption).

TRIPLE DES: Block cipher formed from the DES cipher by using it three times. Triple DES is also known as TDES or 3DES, however, there are variations of TDES which use two different keys (2TDES) and three different keys (3TDES) therefore the non-standard abbreviation 3DES is considered confusing and should be avoided. In general TDES with three different keys (3TDES) has a key length of 168 bits: three 56-bit DES keys (with parity bits 3TDES has the total storage length of 192 bits), but due to the meet-in-the-middle attack the effective security it provides is only 112 bits. 2TDES is weaker and not recommended because two of the three keys used are identical.

VPN: Protected information system link utilizing tunneling, security controls, and end-point address translation giving the impression of a dedicated line.

WPA2: Wi-Fi Protected Access (WPA) is used to secure wireless (Wi-Fi) computer networks. WPA2 implements the full IEEE 802.11i standard and replaces Wired Equivalent Privacy (WEP).

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 680-03: Encryption

6.2 RELATED DOCUMENTS

Information Technology Standard 680-01S1: Information Protection

Signed by Eugene J. Akers, Ph.D., Assistant Director

Revision History

Version	**Release Date**	**Comments**
Original	05/23/2006	